日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００１年　７月１８日

出願番号
Application Number: 特願２００１－２１７７１０

[ST. 10/C]: ［ＪＰ２００１－２１７７１０］

出願人
Applicant(s): エフ・ディー・ケイ株式会社

２００３年　８月　７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０６３５６６

【書類名】　特許願
【整理番号】　IP01401
【あて先】　特許庁長官　殿
【国際特許分類】　H03K　3/84
【発明者】
【住所又は居所】　東京都港区新橋５丁目３６番１１号　いわき電子株式会社内
【氏名】　山本　博康
【発明者】
【住所又は居所】　東京都港区新橋５丁目３６番１１号　いわき電子株式会社内
【氏名】　曽我　竜司
【発明者】
【住所又は居所】　東京都港区新橋５丁目３６番１１号　いわき電子株式会社内
【氏名】　清水　隆邦
【発明者】
【住所又は居所】　東京都港区新橋５丁目３６番１１号　いわき電子株式会社内
【氏名】　鯉渕　美佐子
【特許出願人】
【識別番号】　390022792
【氏名又は名称】　いわき電子株式会社
【代理人】
【識別番号】　100067046
【弁理士】
【氏名又は名称】　尾股　行雄
【電話番号】　03-3543-0036

【選任した代理人】

【識別番号】　100096862

【弁理士】

【氏名又は名称】　清水　千春

【電話番号】　03-3543-0036

【手数料の表示】

【予納台帳番号】　008800

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　乱数発生装置

【特許請求の範囲】

【請求項１】　二つの入力信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップと、

前記入力信号の位相を調整する位相調整部と、

前記入力信号によるフリップ・フロップ出力の０または１の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、

前記位相調整部は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備え、位相調整幅の拡大と位相調整時間の短縮を図ったことを特徴とする乱数発生装置。

【請求項２】　前記粗調整手段および微調整手段は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで、それぞれ構成されることを特徴とする請求項１に記載の乱数発生装置。

【請求項３】　二つの入力信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップと、

前記入力信号の位相を調整する位相調整部と、

前記入力信号によるフリップ・フロップ出力の０または１の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、

前記位相調整部は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで構成されており、

且つ、０または１の出現率の正規分布と前記繰り返し周期内における０または１の出現回数を対比し、当該出現回数が対応する前記正規分布の位置に応じて前記可逆カウンタのカウント数を可変する制御回路を備え、位相調整時間の短縮を図ったことを特徴とする乱数発生装置。

【請求項４】　電源投入時から一定期間、前記繰り返し周期を通常動作時の繰り返し周期より短くする初期制御回路を備えることを特徴とする請求項１から請求項３までの何れかに記載の乱数発生装置。

【請求項５】　前記フリップ・フロップの双方の入力ラインにノイズ発生源とノイズ／位相変換器を付加したことを特徴とする請求項１から請求項４までの何れかに記載の乱数発生装置。

【請求項６】　前記フリップ・フロップの何れか片方の入力ラインにノイズ発生源とノイズ／位相変換器を付加したことを特徴とする請求項１から請求項４までの何れかに記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の０または１の出現率が一定になるようにした乱数発生装置に関し、特に効率的な位相調整手段に関するものである。

【０００２】

【従来の技術】

高度な科学技術計算やゲーム機、或いは暗号処理等には乱数の使用が不可欠であり、近年、一様性を有し、乱数出現の規則性、前後の相関性、周期性を有しない高性能な乱数発生装置の需要が益々増大してきている。

【０００３】

そして、このような乱数発生装置として、フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の０または１の出現率が一定になるようにした乱数発生装置が好適である。係る乱数発生装置は、全てデジタル回路で構成できるためＬＳＩ化への対応が容易で、生産性、コスト性に優れることから、今後の市場規模は極めて膨大である。

【０００４】

【発明が解決しようとする課題】

ところで、前記乱数発生装置にあっては、通常、フリップ・フロップ出力（乱

数）の０または１の出現数を監視して、その出現率が、例えば、５０パーセントに収束するよう、二つ入力信号の位相差を遅延回路にて自動調整する、いわゆる、フィードバック制御による位相調整手段が採用されるが、特に前記用途に対しては高速性や高性能（高精度）を要求されることから、前記フィードバック制御の応答性が重要な課題であり、所定の出現率に効率良く、且つ高精度で収束できる位相調整手段の実現が望まれている。

【０００５】

本発明は、前記要望を満足できる高速で高性能な乱数発生装置を提供することを目的としている。

【０００６】

【課題を解決するための手段】

二つの入力部に入力される信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップとして、例えば、Ｄタイプフリップ・フロップが公知である。

このＤタイプフリップ・フロップは、図８に示すように、入力部となるクロック端子ＣＬＫとデータ端子Ｄを有し、ＣＬＫ入力信号の立ち上がり時のデータ端子Ｄの状態によって出力（Ｑと／Ｑ）の状態が確定する、所謂エッジトリガ型のフリップ・フロップである。

【０００７】

ここで、図９（ａ）、若しくは図９（ｂ）の状態からＣＬＫ信号の立ち上がり時間とＤ信号の立ち上がり時間の差（位相差）△ｔを０に近づけていくと、図９（ｃ）に示すように、フリップ・フロップ出力Ｑｎ、／Ｑｎが不確定となる位相差の範囲が存在する。そして、このフリップ・フロップの不確定動作範囲は入力信号のジッタが大きくなる程広くなり、乱数の生成を容易にする。

本発明は、このようなフリップ・フロップの不確定動作を積極的に利用した乱数発生装置である。

【０００８】

すなわち、請求項１に記載の本発明は、二つの入力信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップと、前記入力信号の位相を

調整する位相調整部と、前記入力信号によるフリップ・フロップ出力の０または１の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、前記位相調整部は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備えて構成される。

【０００９】

また、請求項２に記載の本発明は、請求項１に記載の乱数発生装置において、前記粗調整手段および微調整手段は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで、それぞれ構成される。

前記請求項１または請求項２に記載の構成では、位相の祖調整、微調整を行うことにより位相調整範囲の拡大と効率的な位相調整が可能となる。

【００１０】

また、請求項３に記載の本発明は、二つの入力信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップと、前記入力信号の位相を調整する位相調整部と、前記入力信号によるフリップ・フロップ出力の０または１の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、前記位相調整部は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで構成されており、且つ、０または１の出現率の正規分布と前記繰り返し周期内における０または１の出現回数を対比し、当該出現回数が対応する前記正規分布の位置に応じて前記可逆カウンタのカウント数を可変する制御回路を備えて構成される。

本構成では、０または１の出現回数が少ない領域では、遅延出力の切換幅を多くして位相の粗調整を行い、正規分布のセンターに近づくに連れて遅延出力の切換幅を小さくして位相を微調整する。これにより、効率的な位相調整が可能となる。

【００１１】

また、請求項４に記載の本発明は、請求項１から請求項３までの何れかに記載の乱数発生装置において、電源投入時から一定期間、前記繰り返し周期を通常動作時の繰り返し周期より短くする初期制御回路を備えて構成される。

これにより、電源投入から適切な乱数が生成される迄の期間を短縮できる。

【００１２】

また、請求項５に記載の本発明は、請求項１から請求項４までの何れかに記載の乱数発生装置において、前記フリップ・フロップの双方の入力ラインにノイズ発生源とノイズ／位相変換器を付加して構成される。

【００１３】

さらに、請求項６に記載の本発明は、請求項１から請求項４までの何れかに記載の乱数発生装置において、前記フリップ・フロップの何れか片方の入力ラインにノイズ発生源とノイズ／位相変換器を付加して構成される。

請求項５または請求項６に記載の構成では、フリップ・フロップに入力される信号にジッタが発生し、フリップ・フロップの不確定動作範囲が広がる。これにより、一様性を有し、規則性や相関性や周期性を有しないより完全な自然乱数を高速、且つ高精度に生成することができるようになる。

【００１４】

【発明の実施の形態】

以下、図面に基づいて本発明に係る乱数発生装置の実施形態を説明する。

【００１５】

図１に示すように、本発明の第１実施形態に係る乱数発生装置１０は、フリップ・フロップ１と、位相調整部２と、フィードバック回路部３を基本的構成要素としている。

【００１６】

ここで、前記フリップ・フロップ１としては、二つの入力部に入力される入力信号（ＣＬＯＣＫ）の位相差によって出力の状態（“０”または“１”）が確定する機能を有するフリップ・フロップが使用可能であり、本実施形態では、信号入力用にクロック端子ＣＬＫとデータ端子Ｄを備えた図８に示すＤタイプフリッ

プ・フロップを使用している。

【００１７】

また、前記位相調整部２は、直列に接続され、段階的に遅延量が増加する複数の遅延出力を発生する２つの遅延回路１７，１８（第１ディレー１７、第２ディレー１８）とセレクト入力に応じてこの遅延出力の何れか一つを選択する選択回路１９（セレクター１９）と、このセレクト入力を制御する可逆カウンタ１３（第３カウンター１３）で構成され、前記第１ディレー１７と第２ディレー１８の接続点（遅延中間点となる）が第１ノイズ／位相変換器２０を介して前記フリップ・フロップ１のクロック端子ＣＬＫに接続されると共に、セレクター１９の出力が第２ノイズ／位相変換器２１を介してデータ端子Ｄに接続されて、フリップ・フロップ１に入力される二つの信号の立ち上がり時間の位相差を任意に調整できるように構成されている。

【００１８】

また、前記２つのノイズ／位相変換器２０，２１は、前記フリップ・フロップ入力にジッタを生じさせるために、活性状態にある回路素子（例えば、トランジスタ、抵抗、コンデンサ等）で発生する微弱な熱雑音を利用したノイズ発生源２２，２３からのノイズを遅延出力に合成する回路である。これにより、フリップ・フロップ１の不確定動作範囲が広がり、一様性を有し、且つ、規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができるようになる。

尚、このノイズ／位相変換器は、必ずしも、フリップ・フロップ１のＤ端子とＣＬＫ端子の双方に付加されるものではなく、図２に示す乱数発生装置１０のように、フリップ・フロップ１の何れか片方の入力ライン（図２ではＤ端子のみ）に付加するようにしても良く、同様の効果が得られるものである。

【００１９】

また、前記フィードバック回路部３は、第１カウンター１１、第２カウンター１２、レジスター１４、比較器１５、定数設定器１６で構成される。

【００２０】

第１カウンター１１は、入力信号ＣＬＯＣＫから予め決められた繰返し周期［

ＣＬＯＣＫ数（２×ｍ）］を計測し、第２カウンター１２は、この繰り返し周期毎に前記フリップ・フロップ出力の“１”（または“０”）の出現数を計測する。また、レジスター１４は第２カウンター１２のカウント値を繰り返し周期毎に取り込んで保持する。尚、カウント値がレジスター１４にセットされる毎に第２カウンター１２は０にクリアされる。定数設定器１６はフリップ・フロップ出力の“１”（または“０”）の出現率を設定するための比較データを出力する。本実施形態では、前記繰返し周期［ＣＬＯＣＫ数（２×ｍ）］の１／２の値（ｍ）が出力されるように予め設定されている。また、比較器１５はレジスター１４の保持データ（ｎ）と定数設定器１６からの比較データ（ｍ）を比較し、比較結果（ｎ＞ｍ）または（ｎ＝ｍ）または（ｎ＜ｍ）に対応した比較出力を発生する。第３カウンター１３は、前記比較器１５からの比較出力により設定される動作モードにて動作し、そのカウントデータをセレクター１９のセレクト信号として出力する。そして、既述のようにセレクター１９はセレクト信号により選択されたＣＬＯＣＫ信号の所定の遅延信号を出力する。

【００２１】

すなわち、上記構成によれば、レジスター１４の出力データ（ｎ）と、この定数設定器１６からの出力データ（ｍ）の比較出力に応じて第３カウンター１３が繰り返し周期毎にアップ／ダウン動作（例えば、ｎ＞ｍ時はカウントアップ（＋１）、ｎ＜ｍ時はカウントダウン（－１））を行い、比較器１５の比較出力がｎ＝ｍ（ｎ＝ｍ時はカウント動作を停止（±０）し、ＣＬＯＣＫ信号の位相差は一定を維持する）に収束するようにフリップ・フロップ１のデータ端子Ｄに入力されるＣＬＯＣＫ信号の立ち上がり時間を自動的に補正する。具体的には、図９（ｃ）のように、ＣＬＫ信号の立ち上がりとＤ信号の立ち上がりの位相差Δｔが０に近づいていくように制御される。これにより、フリップ・フロップ１の出力に“０”と“１”の出現率が常時５０％に維持された一様性のある１ｂｉｔのシリアル乱数データＯＵＴが得られる。

【００２２】

以上が乱数発生装置１０の基本動作であるが、本実施形態では、前記第１カウンター１１に初期制御回路２４を接続し、電源投入時から一定クロック数だけ、

第１カウンター１１の通常動作時のカウント設定値（２×ｍ）を強制的にｍ＝１とするようにしている。これにより、電源投入時に確率を１／２に効率良く収束することができ、位相調整期間の短縮化が図れるようになる。

【００２３】

次に図３に基づいて本発明の第２実施形態を説明する。

本実施形態の乱数発生装置１０の基本構成は、図１と同様、フリップ・フロップ１と、位相調整部２と、フィードバック回路部３より構成されるが、図１とは位相調整部２の構成が相違している。

【００２４】

即ち、本構成は、第３カウンター１３、第１セレクター１９、第１ディレー１７、第２ディレー１８で成る位相調整回路を微調整手段として用い、各々の遅延出力に第３ディレー３１、第２セレクター３２で成る粗調整手段と第４ディレー３３、第３セレクター３４で成る粗調整手段を付加し、前記第２セレクター３２および第３セレクター３４のセレクト動作を第４カウンター３０の出力にて指定するものである。因みに、微調整用の第１ディレー１７と第２ディレー１８の１ステップ当たりの遅延時間は粗調整用の第３ディレー３１と第４ディレー３３の遅延時間に比べて約１／２０以下に設定されている。また、この第４カウンター３０は比較器１５の比較出力にて制御されるもので、そのカウント動作は第３カウンター１３の場合と同様である。

【００２５】

以下、図４および表１を参照して図３に示した乱数発生装置１０による位相の粗調整動作および微調整動作を説明する。尚、図４は位相調整時の粗調整と微調整の動作範囲を示し、表１はその際の第３カウンター１３と第４カウンター３０の動作テーブルを示している。ここで、微調整範囲は［０～ｒ×（ｇ－１）］、粗調整範囲は［－ｓ×（ｈ）～ｓ×（ｈ－１）］とする。

初期状態において、粗調整用の第４カウンター３０のカウント値（ＳＮ）と微調整用の第３カウンター１３のカウント値（ＲＮ）は共に０とする。初期制御回路２４により電源投入時に第１カウンター１１の（ｍ）を一定クロック数（図４における位相調整幅ｔｄｗ、即ち、２×（２×ｇ＋ｈ）クロック数）だけ強制的

にｍ＝１に制御されるため、この一定期間、第３カウンター１３は比較器１５の比較出力に基づいて２クロック毎にカウント動作（＋１、または±０、または－１）することになる。また、この間、第４カウンター３０は、比較器１５の比較出力と前記第３カウンター１３の状態に基づいてカウント動作（＋１、または±０、または－１）する。

【００２６】

先ず、（１）最終的に調整される位相ポイントが図４中のａ１にある場合は、電源投入時、第３カウンター１３は比較器１５の比較出力（ｎ＜ｍ）により２クロック毎に０から（ｇ－１）までカウントアップする。

第３カウンター１３がＲＮ＝（ｇ－１）にカウントアップすると、次ぎの２クロックで第４カウンター３０が２クロック毎に比較器１５の比較出力（ｎ＜ｍ）と前記第３カウンター１３のＲＮ＝（ｇ－１）の状態を条件として０から（ｈ－２）までカウントアップし、ＳＮ＝（ｈ－２）となる。ここで、ＳＮ＝（ｈ－２）の状態は、図４中で位相設定ポイントａ１に対応する粗調整ステップ位置であり、これに対応する微調範囲は、図４中の（イ）の範囲[０～ｒ×（ｇ－１）]となる。係るカウンター動作中、第３カウンター１３のＲＮ＝（ｇ－１）の状態は初期制御回路２４の制御の基で強制的に保持されている。

次に、第３カウンター１３がＲＮ＝（ｇ－１）、第４カウンター３０がＳＮ＝（ｈ－２）の状態で、比較器１５の比較出力（ｎ＞ｍ）により第３カウンター１３が２クロック毎にカウントダウンして位相設定ポイントａ１に逐次近付いて行き、フリップ・フロップ出力の“１”の出現率が１／２に収束されるように自動的に位相が調整され、最終的に前記位相設定ポイントａ１の位相前後に留まることになる。

【００２７】

また、（２）最終的に調整される位相がａ２の場合は、初期状態において、ＳＮ＝（０）、ＲＮ＝（０）である。第３カウンター１３がＲＮ＝（０）であると、比較器１５の比較出力（ｎ＞ｍ）により、次ぎの２クロックで第４カウンター３０が２クロック毎に（０）から（－２）にカウントダウンし、ＳＮ＝（－２）となる。ここで、ＳＮ＝（－２）の状態は、図４中で位相設定ポイントａ２に対

応する粗調整ステップ位置（－ｓ×２）であり、微調整範囲は、図４中の（ロ）の範囲[０～ｒ×（ｇ－１）]となる。係るカウンター動作中、第３カウンター１３のＲＮ＝（０）の状態は初期制御回路２４の制御の基で強制的に保持されている。

次に、第３カウンター１３がＲＮ＝（０）、第４カウンター３０がＳＮ＝（－２）の状態から、比較器１５の比較出力（ｎ＜ｍ）により第３カウンター１３が２クロック毎にカウントアップして位相設定ポイントａ２に逐次近付いて行き、最終的にフリップ・フロップ出力の“１”の出現率が１／２に収束されるように自動的に調整され、前記位相設定ポイントａ２の位相前後に留まることになる。

【００２８】

次に、（３）初期制御動作により位相設定ポイントがａ１またはａ２に調整された以降の通常動作では、表１に示すように、第３カウンター１３は、ＲＮ＝（０）またはＲＮ＝（ｇ－１）以外の時、第１カウンター１１で設定したｍ（例えばｍ＝２５０）による一定期間（２×ｍのクロック毎）に比較器１５の比較出力に基づくカウント動作（＋１、±０、－１）が行われる。

また、ＲＮ＝（０）の時、第３カウンター１３は、比較器１５の比較出力に基づいて［＋１、±０、ＲＮ（ｇ－１）］のカウント動作を行い、第４カウンター３０は第３カウンター１３がＲＮ（ｇ－１）に移行する時－１される。

また、ＲＮ＝（ｇ－１）の時、第３カウンター１３は、比較器１５の比較出力に基づいて［＋１、±０、ＲＮ（ｇ－１）］のカウント動作を行い、第４カウンター３０は第３カウンター１３がＲＮ＝（０）に移行する時＋１される。

【００２９】

以上のように、先ず始めに、所定の位相まで大まかに位相が調整され（粗調整）、その後、最終的に調整される位相設定ポイントに微調整されて行く。これにより、高精度の位相調整が効率的に行われ、フィードバック制御による位相調整の高速化が可能となる。また、粗調整手段を設けることで、少ない遅延ステップ構成で広い位相調整幅が得られるようになり、位相調整部２を構成する回路部品を削減できる。

【００３０】

【表１】

第３カウンター	比較器	初期動作時（ｍ＝１）		通常動作時（ｍは任意）	
		第３カウンター	第４カウンター	第３カウンター	第４カウンター
RN=(0)	n>m	±０	－１	RN=(g-1)	－１
	n=m	±０	±０	±０	±０
	n<m	＋１	±０	＋１	±０
0<RN<(g-1)	n>m	－１	±０	－１	±０
	n=m	±０	±０	±０	±０
	n<m	＋１	±０	＋１	±０
RN=(g-1)	n>m	－１	±０	－１	±０
	n=m	±０	±０	±０	±０
	n<m	±０	＋１	RN=(0)	＋１

【００３１】

次に、図５～図７に基づいて本発明の第３実施形態を説明する。

ここで、図６は一様性を有した乱数発生装置により乱数を１，０００回出力した時の“１”または“０”の出現回数をプロットした図で、正規分布を示す。図７はこの正規分布をセンター基準に等間隔で８分割し、センターを±０として総計１０個の各分割位置に対して図７中、右端から＋５～－５の重み付けをしたものである。

【００３２】

図５に示す乱数発生装置１０は、図１の乱数発生装置１０における比較器１５の比較形態をマルチに変えると共に、その出力に制御回路４０を接続して構成したものである。本実施形態では、レジスター１４の内容（ｎ）と比較する比較器１５の比較データを、図７に示す正規分布のマルチ分割位置データ（ｍ＋４×ｋ）～（ｍ－４×ｋ）としており、前記出現回数のカウント数が正規分布のどの分割位置に対応するかを即座に出力できるように構成されている。

【００３３】

また、前記制御回路４０は、比較器１５の比較出力（（ｎ＞ｍ＋４×ｋ）～（

ｎ＞ｍ－４×ｋ））より分割位置データに対応する重み付け（－５～＋５）を判断し、それにぞれに応じたカウント数を第３カウンター１３にセットする。第３カウンター１３は重み付けに応じたカウント動作を行い、セレクター１９による遅延出力の切換幅（切換ステップ数）を制御する。例えば、重み付けが（－４）であれば、第３カウンター１３は一回の動作でダウンカウントを４回繰り返し、重み付けが（＋３）であれば、１回の動作でアップカウントを３回繰り返す。また、重み付けが（０）であれば、カウント動作は停止している。

【００３４】

このように、本構成では、“０”または“１”の出現回数が少ない正規分布領域（例えば、図７において出現回数が４５０或いは５５０の近傍）では、重み付けにより遅延出力の切換幅を多くして位相の粗調整を行い、正規分布のセンターに近づくに連れて（図７における出現回数が５００の近傍）遅延出力の切換幅を小さくして位相を微調整する。これにより、効率的な位相調整が可能となる。

【００３５】

以上説明した第１～第３実施形態では、乱数発生用のフリップ・フロップとしてＤタイプフリップ・フロップを用いたが、本発明はこれに限定されるものではなく、これと同等の機能を有するフリップ・フロップであれば使用可能であり、例えば、Ｒ－Ｓフリップ・フロップ等が使用できる。

【００３６】

また、本発明のシリアル型乱数発生装置１０をＰ個並列に配置することにより、Ｐビット構成の並列型乱数発生装置を構成することもできる。

【００３７】

さらに、上記したシリアル型乱数発生装置や並列型乱数発生装置を用いれば、一様性を有し、規則性、相関性、周期性を有さない高速・高性能の確率発生装置を実現することもできる。

【００３８】

【発明の効果】

以上説明したように、本発明によれば、フィードバック制御による位相調整において、位相調整部に粗調整手段と微調整手段を設けたので、効率的な位相調整

が可能となり、乱数発生の高速化が図れる。また、粗調整手段を設けることで、少ない遅延ステップ構成で広い位相調整幅が得られるようになり、その分、回路部品も削減できる。

【００３９】

また、本発明によれば、乱数の０または１の出現率の正規分布と実際の出現回数を対比し、当該出現回数が対応する正規分布の位置に応じて位相調整幅を可変するようにしたので、上記同様に効率的な位相調整が可能となり、乱数発生の高速化が図れる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態に係る乱数発生装置の構成を示す図。

【図２】

本発明の第１実施形態に係る乱数発生装置の図１とは別の構成を示す図。

【図３】

本発明の第２実施形態に係る乱数発生装置の構成を示す図。

【図４】

位相調整時の粗調整と微調整の動作範囲を示す図。

【図５】

本発明の第３実施形態に係る乱数発生装置の構成を示す図。

【図６】

一様性を有する乱数の正規分布を示す図。

【図７】

図６の正規分布を分割し、重み付けした図。

【図８】

Ｄタイプフリップ・フロップを示す図。

【図９】

図８のＤタイプフリップ・フロップの入出力波形を示す図。

【符号の説明】

１　フリップ・フロップ

２　位相調整部

３　フィードバック回路部

１０　乱数発生装置

１３，３０　可逆カウンタ（カウンター）

１７，１８，３１，３３　遅延回路（ディレー）

１９，３２，３４　選択回路（セレクター）

２０，２１　ノイズ／位相変換器

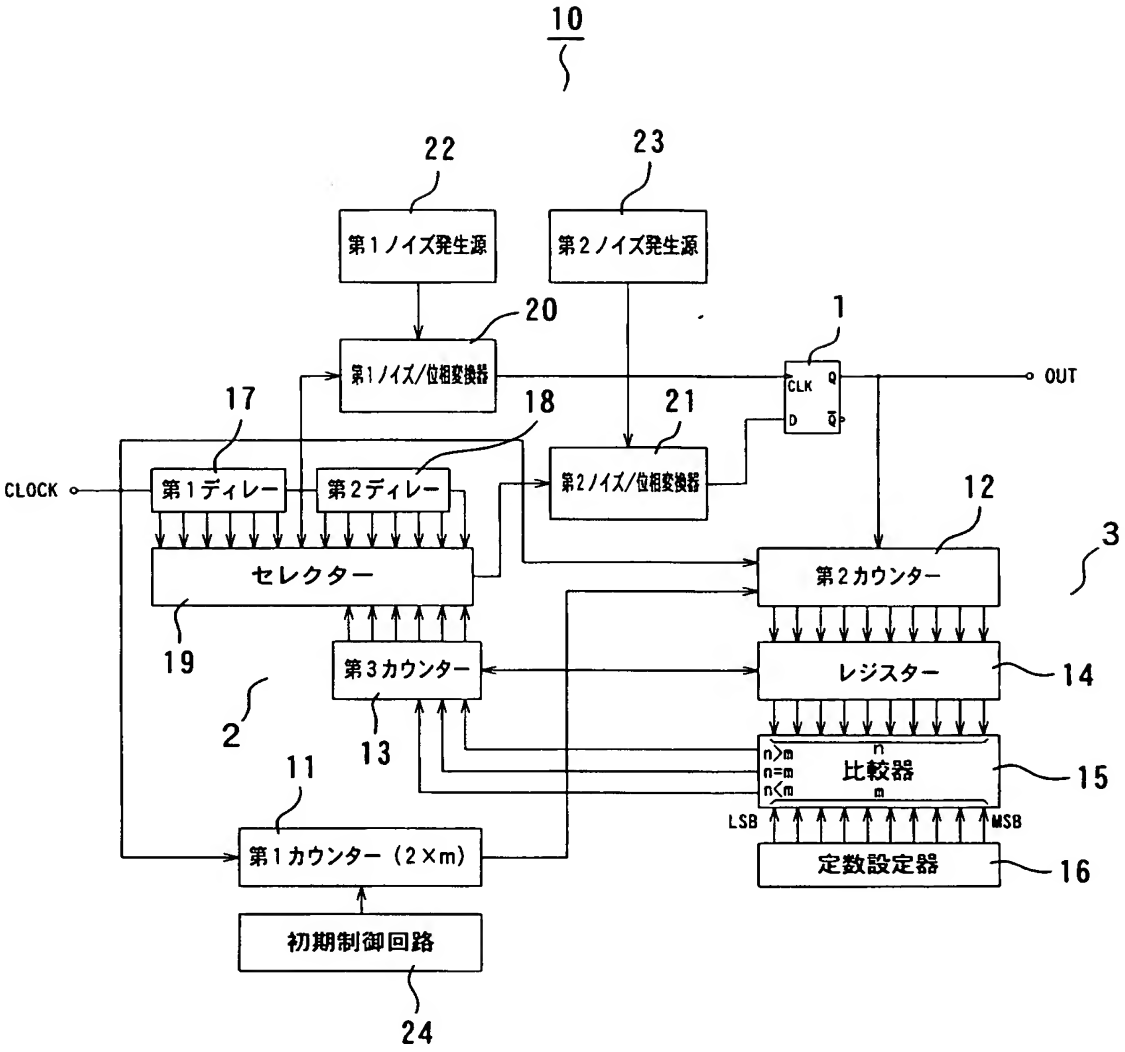
２２，２３　ノイズ発生源

２４　初期制御回路

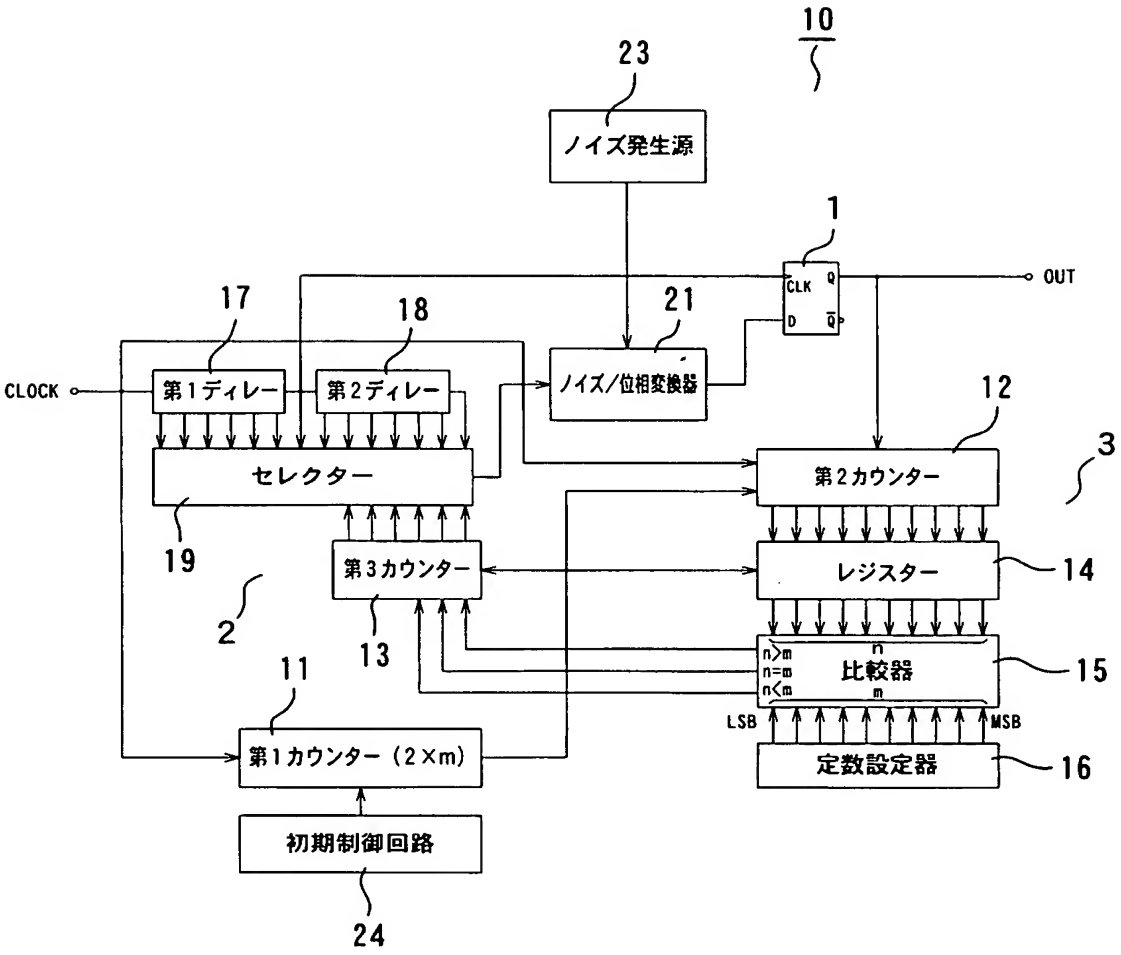
１　制御回路

【書類名】　　図面

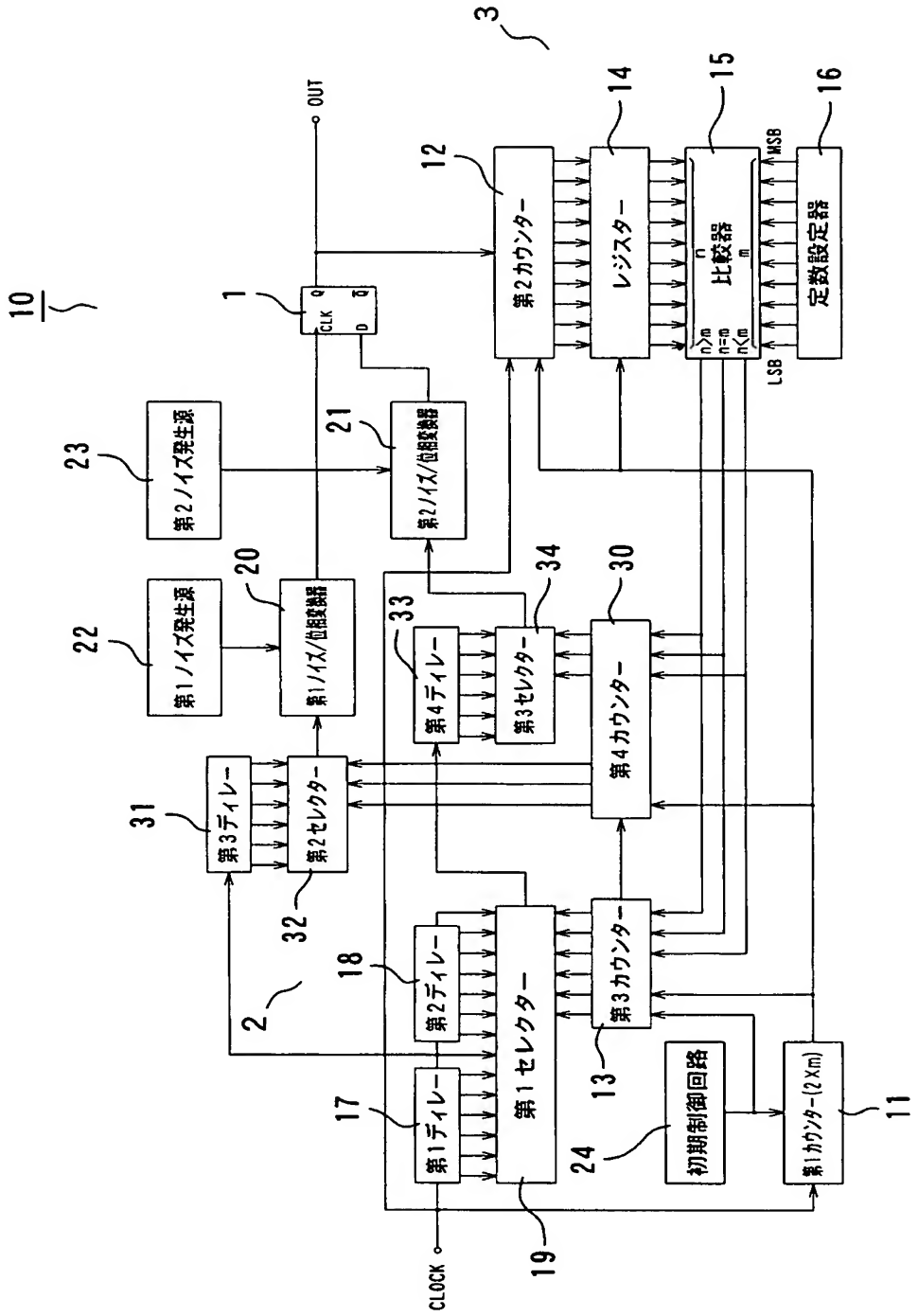
【図１】


10
22
23
第１ノイズ発生源
第２ノイズ発生源
20
1
第１ノイズ/位相変換器
CLK
Q
D
OUT
17
18
21
CLOCK
第１ディレー
第２ディレー
第２ノイズ/位相変換器
12
3
セレクター
第２カウンター
19
第３カウンター
レジスター
14
2
13
n>m
n=m
n<m
n
比較器
m
15
11
LSB
MSB
第１カウンター（２×m）
定数設定器
16
初期制御回路
24

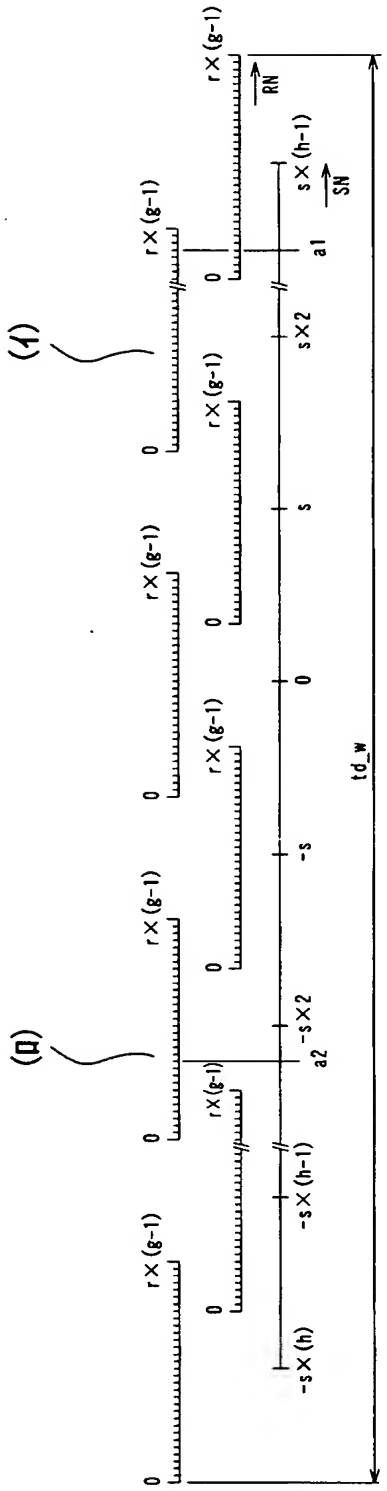
【図２】


10
23
ノイズ発生源
1
CLK
Q
D
Q
OUT
17
18
21
CLOCK
第１ディレー
第２ディレー
ノイズ/位相変換器
12
3
セレクター
第２カウンター
19
第３カウンター
レジスター
14
2
13
n>m
n=m
n<m
n
m
比較器
15
11
LSB
MSB
第１カウンター（２×m）
定数設定器
16
初期制御回路
24

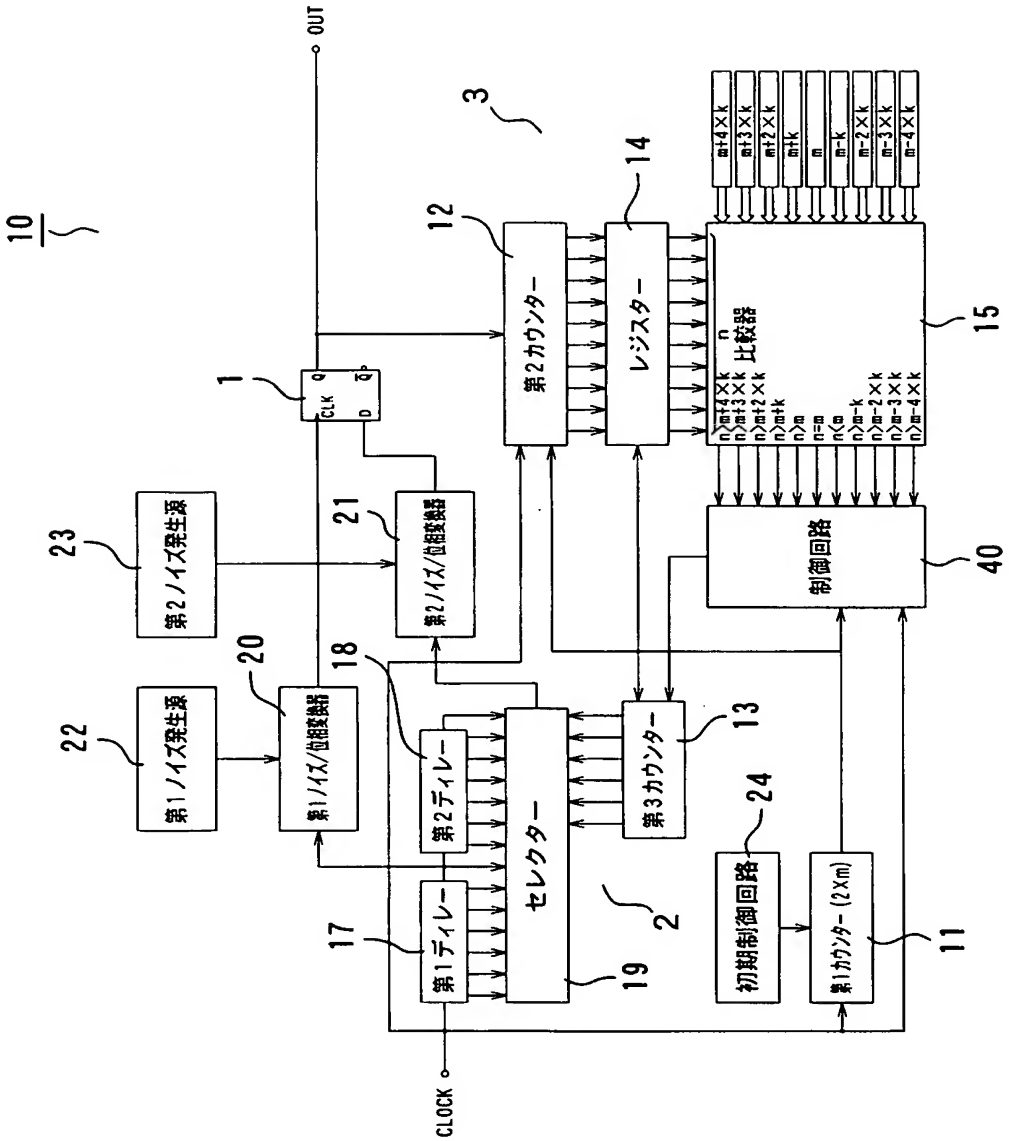
【図３】


10
1
2
3
11
12
13
14
15
16
17
18
19
20
21
22
23
24
30
31
32
33
34
OUT
CLOCK
CLK
D
Q
第2カウンター
レジスター
比較器
定数設定器
MSB
LSB
第2ノイズ発生源
第2ノイズ/位相変換器
第1ノイズ発生源
第1ノイズ/位相変換器
第4ディレー
第3セレクター
第4カウンター
第3ディレー
第2セレクター
第2ディレー
第1セレクター
第3カウンター
第1ディレー
初期制御回路
第1カウンター(2Xm)

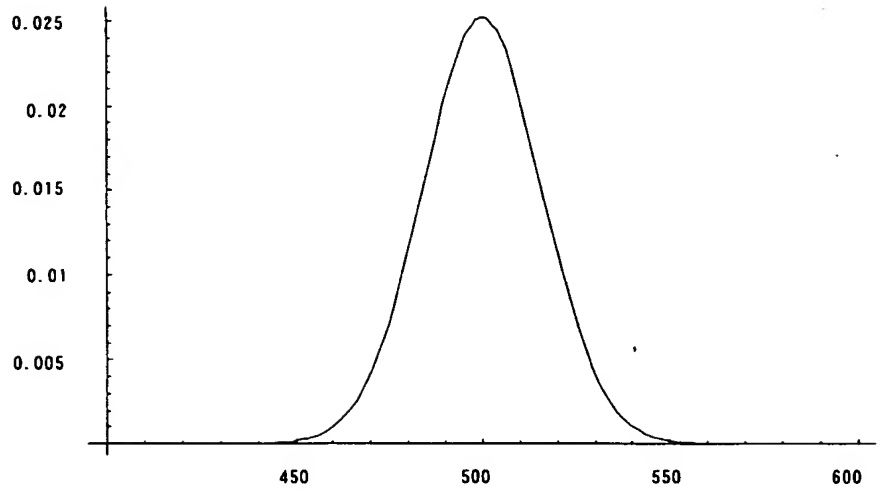
【図４】



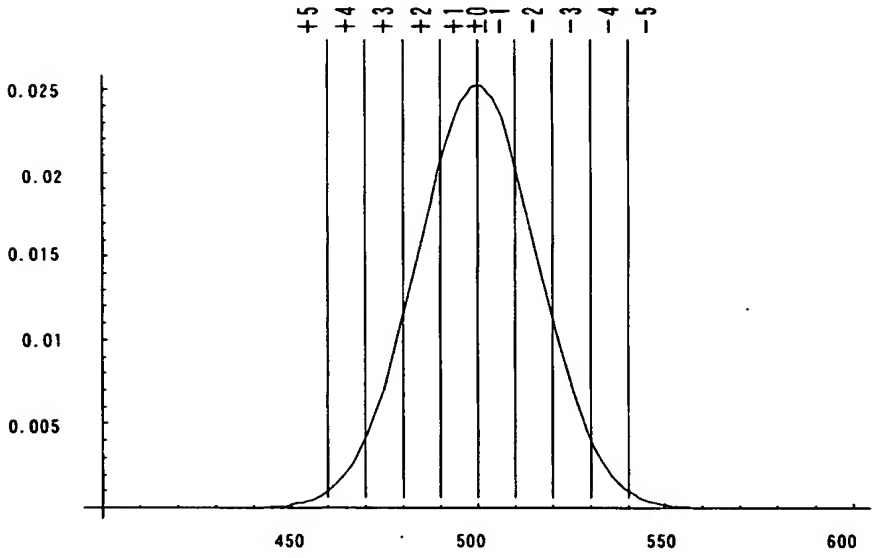
【図５】


10
OUT
3
14
12
m+4×k
m+3×k
m+2×k
m+k
m
m-k
m-2×k
m-3×k
m-4×k
第2カウンター
レジスター
n
比較器
n>m+4×k
n>m+3×k
n>m+2×k
n>m+k
n>m
n=m
n<m
n>m-k
n>m-2×k
n>m-3×k
n>m-4×k
15
1
CLK
Q
D
Q
第2ノイズ発生源
23
21
第2ノイズ位相器
制御回路
40
第1ノイズ発生源
22
20
第1ノイズ位相器
18
第2ディレー
セレクター
第3カウンター
13
24
初期制御回路
17
第1ディレー
2
19
第1カウンター（2×m）
11
CLOCK

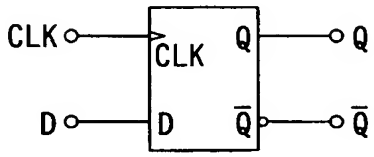
【図６】


0.025
0.02
0.015
0.01
0.005
450
500
550
600

【図７】

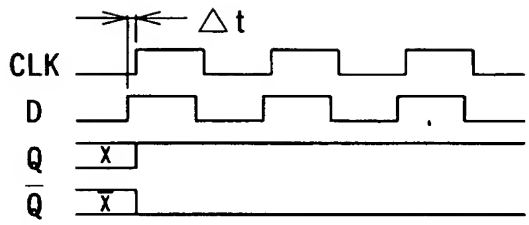

+5
+4
+3
+2
+1
+0
-1
-2
-3
-4
-5
0.025
0.02
0.015
0.01
0.005
450
500
550
600

【図８】

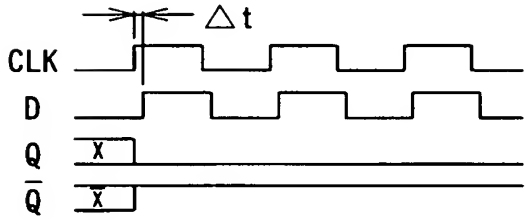

CLK
D
CLK
D
Q
Q̄
Q
Q̄

【図９】

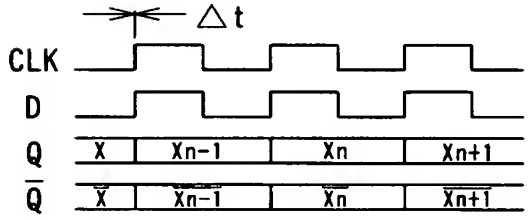
（ａ）



（ｂ）



（ｃ）



【書類名】　　要約書

【要約】

【課題】　一様性を有し、規則性、相関性、周期性を有しない高速・高性能な乱数発生装置を提供する。

【解決手段】　乱数発生装置１０は、二つの入力信号の位相差に応じて出力の状態（０または１）が確定するフリップ・フロップ１と、前記入力信号の位相を調整する位相調整部２と、前記入力信号によるフリップ・フロップ出力の０または１の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部３とで構成される。ここで、前記位相調整部２は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備えている。本構成により、位相調整幅の拡大と位相調整時間の短縮が可能となり、乱数発生の高速化が図れる。

【選択図】　　図３

認定・付加情報

特許出願の番号	特願２００１－２１７７１０
受付番号	５０１０１０５５１７６
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１３年　７月１９日

＜認定情報・付加情報＞

【提出日】　平成13年 7月18日

次頁無

【書類名】　出願人名義変更届（一般承継）
【整理番号】　IP01401
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2001-217710
【承継人】
　【識別番号】　000237721
　【氏名又は名称】　エフ・ディー・ケイ株式会社
【承継人代理人】
　【識別番号】　100067046
　【弁理士】
　【氏名又は名称】　尾股　行雄
　【電話番号】　03-3543-0036
【提出物件の目録】
　【包括委任状番号】　0014478
　【物件名】　閉鎖事項全部証明書　1
　　【援用の表示】　特願２００１－１７０６５２
　【物件名】　履歴事項全部証明書　1
　　【援用の表示】　特願２００１－１７０６５２
【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２００１－２１７７１０
受付番号	５０２００８８８５９２
書類名	出願人名義変更届（一般承継）
担当官	金井　邦仁　　３０７２
作成日	平成１４年　７月１０日

＜認定情報・付加情報＞

【提出日】　平成14年 6月19日

次頁無

特願２００１－２１７７１０

出　願　人　履　歴　情　報

識別番号　　［３９００２２７９２］

１．変更年月日　　１９９０年１１月１３日
［変更理由］　　新規登録
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　いわき電子株式会社

特願２００１－２１７７１０

出　願　人　履　歴　情　報

識別番号　　［０００２３７７２１］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　富士電気化学株式会社

２．変更年月日　　２００１年　１月１６日
［変更理由］　　名称変更
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　エフ・ディー・ケイ株式会社